ABSTRACT OF THE INVENTION

An adaptable cryptographic method and system provides updated digital signature key pairs in a public key system by providing, through a multi-client manager unit, selectable expiry data such as digital signature certificate lifetime data, public key expiry data and private key expiry data as selectable on a per client basis. The multi-client manager unit stores selected public key expiry data and private key expiry data for association with a new digital signature key pair and associates the stored selected expiry data with the new digital signature key pair to facilitate a transition from an old digital signature key pair to a new digital signature key pair.